In re Appln. of Bishop, et al.
App. No. 10/821,379

REMARKS/ARGUMENTS

Claims 5-12 and 43-50 are pending in the present application. Claims 5-12 and 43-50 stand rejected. Claims 5 and 43 have been amended. Claim 6 has been canceled. No claims have been added. Reconsideration of claims 5, 7-12, and 43-50 in light of the present remarks is respectfully requested.

Rejections Under 35 U.S.C. § 102(e)

The Examiner has rejected claims 5-12 and 43-50 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,473,794 to Guheen et al. Applicants respectfully traverse the rejection.

Claim 5 is directed to a method for protecting a network server from being used as the basis of an attack on a network client. Among other elements, amended claim 5 requires "scanning said portion of said network server for particular characters, said particular characters being associated with said selected protocol and removing said particular characters such that the security risk posed by said selected character is reduced." As explained in the specification, in the context of reducing or eliminating undesirable executable code, data provided to the trusted portion of a Web site may be monitored for dangerous characters. In one example, scripting languages, such as JavaScript, are frequently encoded with script instructions placed between angle brackets ("<" and ">"). In this manner, a portion of the network server is scanned for "<" and ">" characters that are associated with the JavaScript protocol and those characters are removed. (*See* Application, pg. 28, lns. 9-29).

In maintaining the rejection of claim 5, the Examiner has directed Applicants to Guheen, col. 75, lns. 13-67, as disclosing the step of "scanning said portion of said network server for particular characters, said particular characters being associated with said selected protocol." (*See* Advisory Action date May 25, 2006, Pg. 2). Applicants respectfully disagree that Guheen, and col. 75, lns. 13-67 in particular, discloses the above-recited element. Rather, Guheen discloses traditional methods of security management to be used in a system for planning and testing components of an existing network frame.

In particular, Guheen discloses eleven types of traditional security management tools. The eleven types of traditional security tools include intrusion detection, platform security, web-based access control, fraud services, mobile code security, e-mail content filtering, application development security toolkits, encryption, public key infrastructure, authentication system, and firewall. (*See* Guheen, col. 75, lns. 13-67). Below, Applicants individually address each of the eleven traditional tools discussed in Guheen.

INTRUSION DETECTION

One type security tool disclosed by Guheen is an intrusion detection mechanism. (*See* Guheen, col. 75, lns. 22-28). The intrusion detection mechanism selectively probes a network's communication system for vulnerabilities used to probe, investigate, and attack a network. Probing a network system for vulnerabilities is not the same as scanning a network server for a particular character where the particular character is associated with a selected protocol and removing said particular character such that the security risk posed by said selected character is reduced, as required by claim 5.

PLATFORM SECURITY

Another type of security tool disclosed by Guheen is a platform security mechanism and Guheen simply discloses that the platform security mechanism provides additional operating system security features. (*See* Guheen, col. 75, lns. 29-31). Guheen does not disclose the specific additional security features of the platform security mechanism and does not disclose that the platform security mechanism scans a network server for a particular character where the particular character is associated with a selected protocol and removes said particular character such that the security risk posed by said selected character is reduced, as required by claim 5.

WEB-BASED ACCESS CONTROL

Yet another type of security tool disclosed by Guheen is a web-based access control mechanism. (*See* Guheen, col. 75, lns. 32-34). The web-based access control mechanism allows for the control and management of user access to web-based applications. The web-based access control mechanism does not scan a network server for a particular character where the particular

character is associated with a selected protocol and remove said particular character such that the security risk posed by said selected character is reduced, as required by claim 5.

FRAUD SERVICES

Guheen also discloses the use of a fraud services mechanism. (*See* Guheen, col. 75, lns. 35-37). The fraud services mechanism verifies the identify of credit card users. The fraud services mechanism does not scan a network server for a particular character where the particular character is associated with a selected protocol and remove said particular character such that the security risk posed by said selected character is reduced, as required by claim 5.

MOBILE CODE SECURITY

Another type of security tool disclosed by Guheen is a mobile code security mechanism. (*See* Guheen, col. 75, lns. 38-40). The mobile code security mechanism protects corporate resources, computer files, confidential information, and corporate assets from a mobile code attach. Guheen does not disclose how this mechanism operates and does not disclose scanning a network server for a particular character where the particular character is associated with a selected protocol and removing said particular character such that the security risk posed by said selected character is reduced, as required by claim 5.

E-MAIL CONTENT FILTERING

Yet another type of security tool disclosed by Guheen is an e-mail content filtering mechanism, which allows organizations to define and enforce email policies. (*See* Guheen, col. 75, lns. 41-43). Again, Guheen does not disclose how the e-mail content filtering mechanism operates and does not disclose scanning a network server for a particular character where the particular character is associated with a selected protocol and removing said particular character such that the security risk posed by said selected character is reduced, as required by claim 5.

APPLICATION DEVELOPMENT SECURITY

Guheen also discloses the use of an application development security toolkit, which allows programmers to integrate privacy, authentication, and additional security features into applications

using a cryptography engine and toolkit. (*See* Guheen, col. 75, lns. 44-47). Using a cryptographic engine is not the same as scanning a network server for a particular character where the particular character is associated with selected protocol and removing said particular character such that the security risk posed by said selected character is reduced, as required by claim 5.

ENCRYPTION

Another type of security tool disclosed by Guheen is an encryption mechanism. (*See* Guheen, col. 75, lns. 48-53). The encryption mechanism provides confidential communications to prevent the disclosure of sensitive information as it travels over a network and is used for conducting business over an unsecured channel, such as the internet. The encryption mechanism does not scan a network server for a particular character where the particular character is associated with selected protocol and remove said particular character such that the security risk posed by said selected character is reduced, as required by claim 5.

PUBLIC KEY INFRASTRUCTURE

Yet another type of security tool disclosed by Guheen is a public key infrastructure mechanism. (*See* Guheen, col. 75, lns. 54-59). The public key infrastructure mechanism provides public-key encryption and digital signature services. The purpose of the public key infrastructure is to manage keys and certificates. The public key infrastructure does not scan a network server for a particular character where the particular character is associated with selected protocol and remove said particular character such that the security risk posed by said selected character is reduced, as required by claim 5.

AUTHENTICATION

Another type of security tool disclosed by Guheen is an authentication system that provides a business with the ability to accurately know who they are conducting business with. (*See* Guheen, col. 75, lns. 60-62). The authentication system does not scan a network server for a particular character where the particular character is associated with selected protocol and remove said particular character such that the security risk posed by said selected character is reduced, as required by claim 5.

FIREWALL

The last security tool disclosed by Guheen is a standard firewall that protects against theft, loss, or misuse of important corporate information. Again, Guheen only discusses firewalls in general terms and does not disclose how the firewall operates and further does not disclose that the firewall scans a network server for a particular character where the particular character is associate with selected protocol and removes said particular character such that the security risk posed by said selected character is reduced, as required by claim 5.

The eleven types of security tools discussed above are the only types of security tools disclosed in Guheen. None of these security tools discloses the step of "scanning said portion of said network server for particular characters, said particular characters being associated with said selected protocol and removing said particular characters such that the security risk posed by said selected character is reduced." In order to anticipate a claim, a single source must contain all the elements of the claim. *Hybritech Inc. v. Monoclonal Antibodies, Inc.*, 802 F.3d 1367, 1379, 231 U.S.P.Q. 81, 90 (Fed. Cir. 1986). Moreover, the single source must disclose all of the claimed elements "arranged as in the claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989). Under 35 U.S.C. § 102, missing elements may not be supplied by the knowledge of one skilled in the art of the disclosure of another reference. *Structural Rubber Prods. Co. v. Park Rubber Co.*, 749 F.2d 707, 716, 223 U.S.P.Q. 1264, 1271 (Fed. Cir. 1984).

As noted above, Guheen fails to disclose, teach, or suggest "scanning said portion of said network server for particular characters, said particular characters being associated with said selected protocol and removing said particular characters such that the security risk posed by said selected character is reduced," as required by claim 5. As a result, Applicants respectfully submit that claim 5 is patentable over Guheen. Additionally, claims 7-12 depend from claim 5, and include all the elements of claim 5. Therefore, Applicants respectfully submit that claims 7-12 are also patentable over Guheen.

Claim 43 is directed to a computer-implemented method for protecting a network server from being used as the basis for an attack on a network client. Similar to claim 5, among other

elements, claim 43 requires "scanning a portion of said network server for particular characters associated with a protocol" and "removing said particular characters such that the security risk posed by said selected character is reduced." In maintaining the rejection of claim 43 the Examiner has directed Applicants to Guheen, col. 75, lns. 13-67, as teaching the step of "scanning said portion of said network server for particular characters, said particular characters being associated with said selected protocol." (*See* Advisory Action date May 25, 2006, Pg. 2). Applicants respectfully disagree that Guheen discloses, teaches, or suggests the above-cited element.

As noted above with respect to claim 5, Guheen fails to disclose, teach, or suggest "scanning a portion of said network server for particular characters associated with a protocol" and "removing said particular characters such that the security risk posed by said selected character is reduced" as required by claim 43. As a result, Applicants respectfully submit that claim 43 is patentable over Guheen. Additionally, claims 44-50 depend from claim 43, and include all the elements of claim 43. Therefore, Applicants respectfully submit that claims 44-50 are also patentable over Guheen.

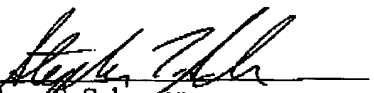
In re Appln. of Bishop, et al.
App. No. 10/821,379

CONCLUSION

In view of the foregoing remarks, Applicants respectfully submit that all of the claims in the Application are in allowable form and that the Application is in condition for allowance. If, however, any outstanding issues remain, Applicants respectfully urge the Examiner to telephone Applicants' undersigned attorney so that the same may be resolved and the Application expedited to issue. Applicants respectfully request the Examiner to indicate all claims as allowable and to pass the Application to issue.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Stephen T. Scherer
Registration No. 45,080

Please recognize our Customer No. 1923 as our correspondence address.

227 West Monroe Street
Chicago, IL 60606-5096
Phone: 312.372.2000
Facsimile: 312.984.7700
Date: November 6, 2006

CHI99 4685200-1.037355.0239